(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 July 2005 (28.07.2005)

PCT

(10) International Publication Number
WO 2005/069089 A2

(51) International Patent Classification[7]: G05B 9/03

(21) International Application Number:
PCT/IB2005/050701

(22) International Filing Date: 13 January 2005 (13.01.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04300018.1 13 January 2004 (13.01.2004) FR

(71) Applicant *(for all designated States except US)*: **RENAULT S.A.S.** [FR/FR]; 13, 15 quai Alphonse le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BOUTIN, Samuel** [FR/FR]; 10 chemin de la chapelle, F-78114 MAGNY-LES-HAMEAUX (FR).

(74) Agent: **DAVIES, Owen**; Renault Technocentre, TCR GRA 1 55-SCE 0267, 1 avenue du Golf, F-78288 Guyancourt (FR).

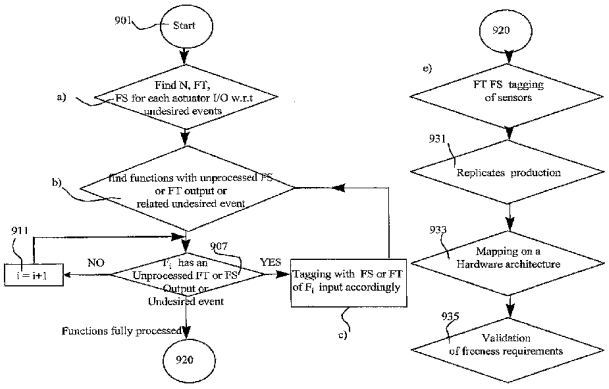
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DESIGN OF SAFETY CRITICAL SYSTEMS



(57) Abstract: A method is disclosed of producing a system architecture comprising a plurality of electrical devices connected to each other, said system preferably comprising a fault tolerant system, the method including: a) identifying a set of undesirable events and ascribing to each of said undesirable events an indicator of their severity; b) associating where possible each said undesirable event with one or more actuators of said system architecture; c) developing a functional specification of an initial architecture proposed for implementation of said system architecture, said functional specification of said initial architecture including datafiow for and between components thereof, said components comprising for example sensors or actuators; d) refining on said functional specification the fault tolerance requirements associated with the severity of each said undesirable event and issuing refined fault tolerance requirements of said functional specification; e) producing replicates in said functional specification together with attached indicators of independence of said replicates, said indicators reflecting said refined fault tolerance requirements; f) defining a hardware structure for said system architecture, e.g. a series of electronic control units connected to each other by networks; g) mapping of said functional specification onto said hardware structure; and h) verifying automatically that said indicators of independence are preserved during mapping.

WO 2005/069089 A2